

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Google drive account and email address

gino.190719@gmail.com, stored at premises controlled
by Google, as further described in Attachment A

Case No. 22-978M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 8, 2022 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____

Hon. Nancy Joseph

(United States Magistrate Judge)

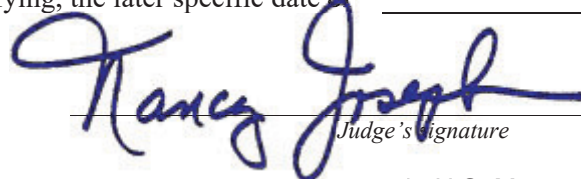
☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

8/25/2022 @ 12:36p.m.

City and state: Milwaukee, Wisconsin



Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Google drive account and email address that is stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain View, California.

Target Account: gino.190719@gmail.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of January 1, 2020 to the present:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

f. All communications, in whatever form, and other information from Google Hangouts associated with the account;

g. All information and documents from Google Drive associated with the account;

h. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google; and

i. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of state and federal controlled substances laws and money laundering laws including Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956 and 1957, and other related offenses involving Luis Ernesto OCEGUERA TIRADO since January 1, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: the sale of illegal drugs and the laundering of proceeds of drug sales.

The identity of the person(s) who created or used the Google Account, including records that help reveal the whereabouts of such person(s);

- a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- d. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Google drive account and email address
gino.190719@gmail.com, stored at premises controlled
by Google, as further described in Attachment A

Case
No.22-978M
(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 U.S.C. §§ 841(a)(1) & 846 See Attached Affidavit.
18 U.S.C. §§ 1956 & 1957

Offense Description

The application is based on these facts:
See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

KELLEN WILLIAMS

Digitally signed by KELLEN WILLIAMS
Date: 2022.08.24 12:34:05 -05'00'

Applicant's signature

DEA SA Kellen Williams

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means)

Date: 8/25/2022

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANTS**

I, Kellen J. Williams, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a Google account that is stored at premises controlled by Google, Inc. (“Google”) an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration (DEA), having been so employed since September 2012. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Sections 2516(1)(e), 1956, and 1957, and Title 21, United States Code, Sections 841(a)(1), 843(b), 846, 856, 952, and 963. I have received specialized training on drug identification, surveillance operations, firearms handling, report writing techniques, confidential source handling, Title III wire interceptions and execution, search warrant execution, arrest procedures, and court proceedings.

3. Based on my training, experience, and participation in drug trafficking and computer related investigations, I know and have observed the following:

- a. I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin as well as in other areas of the United States and internationally;
- b. I am familiar with the coded language utilized over the telephone and other electronic communications to discuss drug trafficking and know that the language is often limited, guarded and coded. I also know the various code names used to describe controlled substances;
- c. I know drug dealers often put telephones in the names of others (nominees) in order to distance themselves from telephones that they use to facilitate drug distribution. Because drug traffickers go through many telephone numbers, they often do not pay final bills when they are done using a telephone number and then are unable to put another line in the name of that subscriber;
- d. I know drug traffickers often purchase and/or title assets in fictitious names, aliases or the names of relatives, associates or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;
- e. I know drug traffickers must maintain on-hand large amounts of currency to include currency stored in financial accounts readily accessible in order to maintain and finance their ongoing drug business;
- f. I know it is common for drug traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances. The aforementioned book, records, receipts, notes, ledger, etc., are maintained where the traffickers have ready access to them. These may be in paper form as well as in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;
- g. I know it is common for large-scale drug traffickers to secrete contraband, proceeds of drug sales and records of drug transactions in secure locations within their residences, their businesses and/or other locations over which they maintain dominion and control, for ready access and to conceal these items from law enforcement authorities;
- h. I know it is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and

gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences, businesses or other locations over which they maintain dominion and control, as well as in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;

- i. I know large-scale drug traffickers often use electronic equipment such as telephones (land-lines and cell phones), pagers, computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;
- j. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency;
- k. I know drug traffickers commonly maintain addresses or telephone numbers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization in papers and books as well as in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;
- l. I know drug traffickers take or cause to be taken photographs or videos of themselves; their associates, their property and their drugs. These traffickers usually maintain these photographs or videos in their possession, often in digital form on computers, Smartphones, cellphones, and other electronic media or electronic storage devices;
- m. I am familiar with computers, cellular telephones, Smartphones, pagers and their uses by drug traffickers to communicate with suppliers, customers, and fellow traffickers; Drug traffickers use these devices to record their transactions and aspects of their lifestyle related to drug dealing, whether in the form of voicemail, email, text messages, video and audio clips, floppy disks, hard disk drives, thumbnail drives, CD's, DVD's, optical disks, Zip disks, flash memory cards, Smart media and any data contained within such computers or cellular telephones, electronic storage media and other settings particular to such devices; I know that such devices automatically record aspects of such communications, such as lists of calls and communications, and any particularized identification assigned to those source numbers or email addresses by the owner of the devices; and

- n. I know the following information can be retrieved to show evidence of use of a computer or Smartphone to further the drug trade: system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; computer media and any data contained within such media; operating system software, application or access program disks, manuals, books, brochures, or notes, computer access codes, user names, log files, configuration files, passwords, screen names, email addresses, IP addresses, and SIM cards.

4. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956 and 1957, have been committed by the user of **gino.190719@gmail.com** (**TARGET ACCOUNT**), Gino David AHUMADA PINEROS. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses.

6. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated; *see* 18 U.S.C. § 2711(3)(A)(i).

II. PROBABLE CAUSE

7. On August 20, 2020, the Federal Bureau of Investigation (FBI) National Threat Operations Center received an online tip via tips.fbi.gov regarding potential international drug trafficking and tax evasion. The tip identified Dwight CLAYTON and stated that individuals are using a business called S&C Trucking LLC to hide proceeds in Milwaukee, Wisconsin. The tip stated a second unidentified person owes a large sum of money for income taxes and owes child support and started a business to get paid “under the table” from a source. The tip stated this second person ran income through that source and uses his girlfriend’s accounts to hide profits from drug trafficking. The tip further stated that this second person is involved in drug trafficking with the people who operate S&C Trucking LLC, 1918 East Lafayette Place #309, Milwaukee, Wisconsin, and is a co-owner of the business. The tipster identified this person as Dwight CLAYTON. The tip stated that the business is registered “with the DOT under a different address which is a home.” The tipster further reported that CLAYTON had been sent to prison for federal drug charges in the past. According to the tip, CLAYTON and the second person lived lavish lifestyles and clearly lived beyond their means.

8. A search of Wisconsin Department of Financial Institutions records revealed that Dwight CLAYTON is the registered agent of S&C Trucking LLC. The LLC address listed for the business is 9736 West Tower Avenue, Milwaukee, Wisconsin. Case agents conducted surveillance at this location on several occasions and have never seen a person or vehicle come or go from the residence. Additionally, cameras are mounted on the exterior of the residence and all of the window blinds are closed. I am aware, based on my training and experience, that drug traffickers frequently maintain “stash” houses which are residences used to store drugs prior to distribution and/or to store proceeds of drug sales after distribution. These residences typically have little

vehicle or pedestrian traffic so as to avoid drawing attention to the house. Additionally, cameras are often mounted to the exterior of “stash” houses to allow the drug trafficker to observe if the residence is being approached by Police or rival drug traffickers.

9. On October 20, 2020, Texas Department of Public Safety investigators were conducting surveillance at a suspicious business in Pharr, Texas. Investigators observed an open overhead garage door at the business warehouse and observed a pallet containing several boxes sitting next to a pickup truck in the business. The rest of the warehouse appeared to be empty. A short time later, a truck belonging to Estes Express Lines arrived, loaded the pallet onto a truck, and left the business. Investigators maintained surveillance until the truck arrived at the Estes Express Lines property. Investigators subsequently approached the employees of the company and inquired about the pallet. Investigators were provided with the bill of lading related to the shipment. The bill of lading indicated that the pallet contained 492 pounds of optical cable and was being shipped from Dixie Cable, 2003 North Veterans Boulevard, Suite 18, Pharr, Texas 78577 to Raul Gallegos, 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. The shipper name was listed as Carlos Trevino with phone number (956) 996-2424. The recipient was listed as Raul Gallegos with phone number (657) 261-1934. Investigators conducted a K-9 sniff of the pallet and received a positive alert for the presence of controlled substances. A subsequent search of the pallet revealed approximately 60 kilograms of cocaine concealed within the boxes on the pallet.

10. Shipping records revealed that three prior shipments had been sent from Pharr, Texas to 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. Two of those shipments had been picked up at the shipping company and one had been delivered on August 14, 2020, to 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee,

Wisconsin 53212. Case agents obtained surveillance video from North Shore Bank which showed that on August 14, 2020, Dwight CLAYTON arrived at the side of the business at 1850 North Martin Luther King Jr. Drive, driving a black Dodge Ram 2500 pickup. The bed of the pickup was empty upon his arrival. A short time later, a box truck driven by the shipping contractor arrived and parked on the side of the business. CLAYTON was observed positioning the Dodge Ram near the shipping company vehicle. A short time later, CLAYTON drove away from the area. The bed of the Dodge Ram now contained what appeared to be a shipping pallet. This pallet was similar in appearance to the pallet seized in Pharr, Texas on October 20, 2020.

11. A search of Wisconsin Department of Financial Institutions records revealed that Peachy Clean Commercial and Construction Cleaning LLC lists its office address as 1850 North Doctor Martin Luther King Jr. Drive #210, Milwaukee, Wisconsin 53212. The registered agent is Ronny Thompson. Numerous law enforcement database searches identified Ronny Thompson's phone number as (414) 803-9676.

12. Administrative Subpoenas were sent to AT&T for records related to (414) 469-6235, the number used by Dwight CLAYTON. The phone is subscribed to Dwight CLAYTON at 9736 West Tower Avenue, Milwaukee, Wisconsin. An analysis of the records for (414) 469-6235 revealed that CLAYTON was in contact with (414) 803-9676, the number used by Ronny Thompson, 153 times from March 5, 2020, through October 8, 2020. An examination of records for (414) 469-6235 also revealed that CLAYTON was in regular and frequent contact with other phones known to be used by drug traffickers in the Milwaukee area.

13. A search of Public Access to Court Electronic Records (PACER) records revealed that on April 12, 2005, Dwight CLAYTON was convicted in Case # 04-CR-66 of Conspiracy to Possess with Intent to Distribute Five Kilograms of Cocaine and Money Laundering. CLAYTON

was sentenced to 108 months of imprisonment on each count with the sentences to run concurrently.

14. On November 2, 2020, the Honorable William E. Duffin, United States Magistrate Judge in the Eastern District of Wisconsin, signed a tracking warrant for a silver 2015 Kia Optima, bearing Wisconsin license plates ACV-2064, known to be driven by Dwight CLAYTON. On November 24, 2020, case agents observed that the Kia left 9736 West Tower Avenue, Milwaukee, Wisconsin, and travelled directly to a vacant lot in the 4700 block of South Packard Avenue, Cudahy, Wisconsin. Case agents responded to that area to conduct surveillance of the Kia. At 3:27 p.m., case agents observed that the Kia had travelled to the parking lot of a BMO Harris Bank located at 4677 South Packard Avenue, Cudahy, Wisconsin. Case agents conducted surveillance of the Kia and observed CLAYTON in the driver's seat and a second unidentified male in the front passenger seat. The second male appeared to be looking down at the passenger-side floorboard. At 3:35 p.m., the Kia drove out of the BMO Harris parking lot and drove back to the 4700 block of South Packard Avenue. The Kia did a U-turn and pulled to the curb on the south side of the street. Case agents observed the unidentified male exit the front passenger seat and retrieve a small rolling suitcase and a small duffel bag from the vehicle. The male then entered the JP Morgan Chase Bank at 4702 South Packard Avenue, Cudahy, Wisconsin. CLAYTON drove the Kia out of the area and was not followed.

15. The unidentified male approached a teller window and appeared to be conducting a lengthy transaction. At 4:34 p.m., the male exited the bank and stood in front of the bank looking at his cellular phone. At 4:42 p.m., a vehicle displaying an Uber sticker arrived in front of the bank. The male opened the rear cargo area of the vehicle and placed the suitcase and the duffel bag into the vehicle. Case agents followed the vehicle to the Hilton Garden Inn – Milwaukee

Airport, 5890 South Howell Avenue, Milwaukee, Wisconsin, where the male exited the vehicle and entered the hotel.

16. Case agents interviewed employees at the JP Morgan Chase Bank who stated that the male had made a large cash deposit, but provided no additional information about the transaction. A subpoena served on JP Morgan Chase later revealed that the male had deposited \$169,650 in United States currency to an account held by Redzien LLC, a business organized in the State of Florida. The authorized signers on the account are Kevin MATHIS and Hector Manuel TERAN-VARGAS. Banking records for this account show that the account was opened on September 23, 2020. A search of Florida corporation records identified the registered agent for Redzien LLC as Kevin MATHIS, of 10870 West Sample Road # 4504, Coral Springs, Florida. The Articles of Organization for Redzien LLC identify MATHIS and Hector M. VARGAS, a.k.a Hector TERAN-VARGAS, as Managers of the LLC. Additional banking records identified MATHIS' phone number as (941) 809-5186 and email address as kmathis193@gmail.com and TERAN-VARGAS' phone number as (832) 212-3490. An Administrative Subpoena served on T-Mobile identified the subscriber to (941) 809-5186 as Conceptual Design & Consulting Srvcs Inc, of 193 Medici Ter, North Venice, Florida, and the customer name as "Mathis" and the subscriber to (832) 212-3490 as "Hector Teran" of 8152 Emerald Forest Court, Sanford, Florida 32771.

17. Banking records revealed that Redzien, LLC had also opened bank accounts at Bank of America, Wells Fargo Bank, and Regions Bank. A review of transactions for these banks, and JP Morgan Chase Bank, identified approximately 106 suspicious transactions totaling \$21,268,257 from June 18, 2020, through March 24, 2021. These transactions occurred in at least twenty-one different states, including Wisconsin. On January 20, 2021, case agents spoke to a representative of Bank of America's Global Financial Crimes Investigations – Anti-Money

Laundrying department. The representative advised that from November 23, 2020, thru January 5, 2021, Kevin MATHIS and Hector TERAN-VARGAS had deposited approximately \$1,000,000 into accounts at Bank of America. Bank of America subsequently closed those accounts due to suspicions that the accounts were being used for money laundering.

18. Records indicate that soon after these deposits are made, money is wired out of the account to brokerage accounts of companies in Mexico and the British Virgin Islands. The brokerage firms receiving these wires have previously been identified as being involved in money laundering in numerous drug trafficking and money laundering investigations being conducted by DEA. Furthermore, case agents have identified a large amount of cryptocurrency deposits and subsequent transactions made by TERAN-VARGAS on the cryptocurrency exchange Binance.

19. Case agents believe, based on the numerous, large cash deposits followed by wire transfers to foreign accounts, travel throughout the United States in furtherance of money laundering, and the lack of a legitimate business purpose for large cash transactions involving Redzien, LLC (a mining business), that Kevin MATHIS and Hector TERAN-VARGAS are involved in laundering of drug proceeds throughout the United States, including in the Eastern District of Wisconsin.

20. On January 28, 2021, the Honorable William E. Duffin, Magistrate Judge in the Eastern District of Wisconsin, signed a federal search warrant authorizing the search of Google account teranhector@gmail.com, used by TERAN VARGAS. As a result of that search warrant, Google provided over 3,641 emails to case agents.

21. During a review of those emails, case agents located a large amount of emails between TERAN VARGAS and the cryptocurrency exchange Binance. In March 2021, an administrative subpoena was sent to Binance, requesting any accounts associated with

teranhector@gmail.com. Binance responded with the requested information, and provided customer information, current assets & wallets, order history, deposit history, withdrawal history, access logs and approved devices for TERAN VARGAS' account 47929920. An analysis of the Binance transactions for TERAN VARGAS's account discovered multiple transactions between TERAN-VARGAS and deposit address 0x94c464f6e1f9b8c26a42926f8f3a27babfb53a34. In April 2021, an administrative subpoena was issued to Binance. Agents discovered that deposit address 0x94c464f6e1f9b8c26a42926f8f3a27babfb53a34 is associated with the Binance account belonging to Gino David AHUMADA PINEROS. This account was registered on January 15, 2018, with email gino.190719@gmail.com (**Target Account**) and phone number +57-3187416449. AHUMADA PINEROS provided his Colombian passport AU285361 and live photo as proof of identity. The identification card had a DOB of 01-19-1989 and Colombian Cedula 1130643913.

22. Analysis of deposit address 0x94c464f6e1f9b8c26a42926f8f3a27babfb53a34 revealed that between May 12, 2020 and November 11, 2021, this account had 105 incoming transfers on the Ethereum blockchain for an approximate total of \$9,485,363 and 64 outgoing transfers for an approximately total of \$9,484,984. The balance in AHUMADA PINEROS' Binance account on or around November 11, 2021, the date the transactions, was effectively \$0.00. Analysis of the activity within the account shows that a large portion of the BTC and USDT¹ deposited into the account was quickly converted to USDT and funds generally move in and out of the account rapidly. Case agents believe the primary purpose of AHUMADA PINEROS' Binance account is to facilitate the DTMLO's money laundering activities by receiving drug

¹ USDT is a stable coin cryptocurrency with a value meant to mirror the value of the U.S. dollar; USDT tokens are backed by offshore banks. Offshore banks offer fewer charges for operation and tax benefits, but they aren't always fully secure like the FDIC-insured US banks

proceeds into the account and moving it quickly to other cryptocurrency accounts for the purpose of money laundering. Case agents believe that on or about November 11, 2021, AHUMADA PINEROS stopped using the Binance exchange platform and switched to a different cryptocurrency exchange.

23. Based on my training and experience as well as my knowledge and information garnered from other money launderers in this case and similar cases, I know cryptocurrency transactions are often utilized to launder the proceeds derived from narcotic traffickers. More specifically, narcotics traffickers in source countries (e.g., Mexico and Colombia) provide narcotics to consumer countries (e.g., the United States). The bulk currency proceeds derived from the sale of these narcotics are then returned to the narcotics traffickers within the source countries utilizing various methods including the use of cryptocurrencies. In this case, the narcotic traffickers often contact brokers, or professional money launderers, who are responsible for collecting the bulk currency within the consumer countries and depositing the currency into the U.S. banking system. The brokers often then pay out the narcotics traffickers in fiat currency within the source countries, minus a commission, and sell the cryptocurrency to a separate “crypto” broker. The commission fee is generally between 3% - 5%. This crypto broker may then conduct a series of cryptocurrency transactions across multiple cryptocurrency exchanges utilizing an array of methods (e.g., cryptocurrency scrambler) in effort to obfuscate the true origin of the money. These crypto brokers often then sell the cryptocurrency in the “black market” in exchange for various fiat currencies. Furthermore, individuals who engage in the laundering of drug proceeds will communicate and send and receive information through electronic communication such as e-mails and chats. In this investigation, case agents are aware that AHUMADA PINEROS is heavily involved in cryptocurrency transactions and would likely receive email confirmation of these

transactions in the **Target Account**. Furthermore, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

24. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

25. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

III. BACKGROUND CONCERNING E-MAIL

26. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google's services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. In addition to email, Google offers its users a number of other online services. A list of those services and their features is available at the following URL: <https://support.google.com/>.

28. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

30. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as

technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

31. This application seeks warrants to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

IV. CONCLUSION

32. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of violations of violations of Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956 and 1957 have been committed by the users of the **TARGET ACCOUNT**. There is also probable cause to search the location described in Attachment A for fruits, evidence and instrumentalities of these crimes further described in Attachment B.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Google drive account and email address that is stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain View, California.

Target Account: gino.190719@gmail.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of January 1, 2020 to the present:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

f. All communications, in whatever form, and other information from Google Hangouts associated with the account;

g. All information and documents from Google Drive associated with the account;

h. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google; and

i. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of state and federal controlled substances laws and money laundering laws including Title 21, United States Code, Sections 841 and 846, and Title 18, United States Code, Sections 1956 and 1957, and other related offenses involving Luis Ernesto OCEGUERA TIRADO since January 1, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: the sale of illegal drugs and the laundering of proceeds of drug sales.

The identity of the person(s) who created or used the Google Account, including records that help reveal the whereabouts of such person(s);

- a. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- b. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- d. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____ [Provider], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of _____ [Provider]. The attached records consist of _____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of _____, and they were made by _____ [Provider] as a regular practice; and

b. such records were generated by _____ [Provider] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of _____ [Provider] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by _____
[Provider], and at all times pertinent to the records certified here the process and system
functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of
the Federal Rules of Evidence.

Date

Signature